CLAIMS

1. A method for storing data records on a database system in which a signing entity is used for signing data records, the method comprising:

receiving a second data record to be stored on a database;

retrieving a first integrity checksum stored with a first data record previous to the second data record;

computing a second integrity checksum for the second data record with a cryptographic method based on a storage key, the retrieved first integrity checksum and the second data record; and

storing the second data record and the second integrity checksum on the database.

2. The method according to claim 1, wherein the storage key is a secret key of public key infrastructure.

3. The method according to claim 1, wherein the retrieved integrity checksum for a first row of the database is a generated initialization vector.

4. The method according to claim 1, wherein the retrieved integrity checksum for a first row of the database is a digital signature of the signing entity.

5. The method according to claim 1, wherein the first integrity checksum is retrieved from a memory of a signing entity.

6. The method according to claim 1, wherein the second integrity checksum is stored on a memory of the signing entity.

7. The method according to claim 1, wherein the integrity checksums comprise a running sequence number.

8. A method for verifying integrity of data records on a database in which a verification entity is used for verifying integrity of data records, the method comprising:

retrieving a second data record to be verified from a first database;

retrieving a second integrity checksum of the second data record;

retrieving a first integrity checksum of a first data record previous to the retrieved second data record;

computing a third integrity checksum for the second data record based on the retrieved second data record, the first integrity checksum, and a storage key; and

comparing the second integrity checksum to the third integrity checksum, wherein the second data record is considered authentic if the second integrity checksum and the third integrity checksums are equal.

9. The method according to claim 8, wherein the storage key is a public key of public key infrastructure.

10. The method according to claim 8, wherein the retrieved integrity checksum for a first row of the database is a generated initialization vector.

11. The method according to claim 8, wherein the retrieved integrity checksum for a first row of the database is a digital signatory of the signing authority.

12. The method according to claim 8, wherein the first integrity checksum is retrieved from a memory of a verification entity.

13. The method according to claim 8, wherein the second integrity checksum is stored on a memory of a verification entity.

14. The method according to claim 8, wherein the integrity checksums comprise a running sequence number.

15. A system for storing data records on a database system in which a signing entity is used for signing data records and a verification entity is used for verifying integrity of data records, wherein the system comprises:

a database configured to store and provide signed data;

a data source configured to provide data records to be stored on the database system;

a signing entity configured to sign data records to be stored on the database system with a second integrity checksum computed based on a second data record, a first integrity checksum of the first data record previous to the second data record to be signed, and a storage key; and

a verification entity configured to verify integrity of chosen data records by computing a computed third integrity checksum based on the second data record, the first integrity checksum of the first data record previous to the second data record, and the storage key, and comparing the computed third integrity checksum to the second integrity checksum stored on the database.

16. The system according to claim 15, wherein the signing entity and verification entity apply public key infrastructure for calculating and verifying the one of the first integrity checksum and the second integrity checksum.

17. A computer program embodied on a computer readable medium, said computer program for storing data records on a database system in which a signing entity is used for signing data records, wherein the computer program performs the following steps when executed in a computer device:

receiving a second data record to be stored on a database;

retrieving a first integrity checksum stored with a first data record previous to the second data record;

computing a second integrity checksum for the second data record with a cryptographic method based on a storage key, the retrieved first integrity checksum and the second data record; and

storing the second data record and the second integrity checksum on the database.

18. A computer program according to claim 17, wherein the storage key is a secret key of public key infrastructure.

19. A computer program according to claim 17, wherein the retrieved integrity checksum for a first row of the database is a generated initialization vector.

20. A computer program according to claim 17, wherein the retrieved integrity checksum for a first row of the database is a digital signatory of the signing entity.

21. A computer program according to claim 17, wherein the first integrity checksum is retrieved from a memory of the signing entity.

22. A computer program according to claim 17, wherein the second integrity checksum is stored on a memory of the signing entity.

23. A computer program according to claim 17, wherein the integrity checksums comprise a running sequence number.

24. A computer program embodied a computer-readable medium for verifying the integrity of data records on a database, wherein the computer program performs the following steps when executed in a computer device:

retrieving a second data record to be verified from a database;

retrieving a second integrity checksum of the second data record to be verified from a database;

retrieving a first integrity checksum of a first data record previous to the retrieved second data record;

computing a third integrity checksum for the second data record based on the retrieved second data record, the first integrity checksum, and a storage key; and

comparing the second integrity checksum to the third integrity checksum, wherein the second data record is considered authentic if the second integrity checksum and the third integrity checksums are equal.

25. A computer program according to claim 24, wherein a storage key is a public key of public key infrastructure.

26. A computer program according to claim 24, wherein the retrieved integrity checksum for a first row of the database is a generated initialization vector.

27. A computer program according to claim 24, wherein the retrieved integrity checksum for a first row of the database is a digital signatory of a signing authority.

28. A computer program according to claim 24, wherein the first integrity checksum is retrieved from a memory of a verification entity.

29. A computer program according to claim 24, wherein the second integrity checksum is stored on a memory of a verification entity.

30. A computer program according to claim 24, wherein the integrity checksums comprise a running sequence number.